

Qubit channels with small correlations

Filippo Caruso¹, Vittorio Giovannetti¹, Chiara Macchiavello², Mary Beth Ruskai³

¹ *NEST CNR-INFM & Scuola Normale Superiore, Piazza dei Cavalieri 7, I-56126 Pisa, Italy*

² *Dip. di Fisica and CNISM “A. Volta”, Unità di Pavia, Via Bassi 6, I-27100 Pavia, Italy*

³ *Department of Mathematics, Tufts University, Medford, MA 02155, USA*

We introduce a class of quantum channels with correlations acting on pairs of qubits, where the correlation takes the form of a shift operator onto a maximally entangled state. We optimise the output purity and show that below a certain threshold the optimum is achieved by partially entangled states whose degree of entanglement increases monotonically with the correlation parameter. Above this threshold, the optimum is achieved by the maximally entangled state characterizing the shift. Although, a full analysis can only be done for the 2-norm, both numerical and heuristic arguments indicate that this behavior and the optimal inputs are independent of $p > 1$ when the optimal output purity is measured using the p -norm.

PACS numbers: 03.67.Hk, 05.40.Ca

I. INTRODUCTION

In usual memoryless channel model successive uses of the communication line have the same noise [1] and can be described as a simple tensor product of channels. Recently, there has been some interest in studying the behavior of these channels with correlations [2, 3] since such channels might be regarded as a small first step in studying the much more complex issue of channels with memory [4, 5, 6, 7, 8, 9]. They can also describe multiple access channels. Thus, one is led to consider a scenario in which with probability $1 - \mu$ qubits encounter only uncorrelated tensor product noise, but with probability μ they experience correlated noise. This situation can be modelled by a channel of the form

$$\Phi = (1 - \mu)\Psi \otimes \Psi + \mu\Gamma_{\text{corr}}, \quad (1)$$

where all the correlations are in the map Γ_{corr} , which need not be a channel itself. Several papers [2, 3] have studied specific examples of this type for which there is a critical value μ_c below which the optimal input is a product state and above which the optimal input is maximally entangled. Recently, Daems [10] showed that this is always the case for a class of channels called “product Pauli”. This is not, however, the most general channel of the form (1), even for a pair of qubits.

In this note, we consider a class of channels with correlations which exhibit quite different behavior. The map we use for Γ_{corr} in (1) is extremely simple; it is simply the non-unital channel which maps every input to a fixed maximally entangled state. We study the optimal output purity, rather than the channel capacity. For our channels, the entanglement of the output input increases continuously with μ until it reaches a critical μ_c , after which the optimal input is always achieved with a maximally entangled state.

Although one is ultimately interested in the effect of correlations on various types of channel capacity, we consider here only the optimal output purity. For channels with some covariance properties [11], one can make an explicit connection between the classical capacity [12] and

the optimal output purity as measured by the minimal output von Neumann entropy. However, that need not hold in general and is not true for the channels considered here. Moreover, the conjecture in [13] about capacity achieved with maximally entangled states depends on the precise form of the channels and is not relevant here.

Roughly speaking, one expects inputs whose outputs are close to pure states to be the least corrupted; however, one can have very noisy channels which map all inputs to a region close to a fixed pure state with little correlation with the input. Nevertheless, the optimal output purity as measured by either the minimal output entropy [14, 15] or the maximal output p -norm [16] is of some interest and has been studied extensively. This is, in part, due to the Shor equivalence [17] established between the conjectured additivity of minimal output entropy and other long-standing additivity conjectures. The hope that the additivity of minimal output entropy could be proved by showing that the maximal output p -norm is multiplicative, at least near $p \approx 1$, as conjectured in [16], was recently shattered by the discovery [18] of counterexamples to the latter for all $p > 1$. Nevertheless, the additivity conjectures remain open and even the multiplicativity conjecture is known to hold in the region $1 < p \leq 2$ for certain classes of channels [19, 20, 21, 22] and in other situations for $p = 2$ [23, 24]. Thus, the optimal output purity remains an object of some interest.

For $p > 1$, the p -norm of a state γ is given by the expression

$$\|\gamma\|_p \equiv [\text{Tr}(\gamma^p)]^{1/p}. \quad (2)$$

One sometimes uses instead, the Rényi entropy [25]

$$S_p(\gamma) \equiv \frac{1}{1-p} \ln \text{Tr}(\gamma^p) = \frac{p}{1-p} \ln \|\gamma\|_p, \quad (3)$$

which is known to converge to the usual von Neumann entropy as $p \rightarrow 1$. The maximal output p -norm of a CPT map Φ denoted $\nu_p(\Phi)$, is the supremum of $\|\Phi(\gamma)\|_p$ over all input density matrices γ , i.e.,

$$\nu_p(\Phi) \equiv \sup_{\gamma} \|\Phi(\gamma)\|_p. \quad (4)$$

The minimal output entropy and Renyi entropy are similarly defined as

$$S_p(\Phi) \equiv \inf_{\gamma} S_p[\Phi(\gamma)], \quad (5)$$

and it is natural to refer to states which achieve the optimum in (4) or (5) as optimal inputs.

This paper is organized as follows. In Section II we describe the class of channels we study and show how covariance properties can be used to reformulate the optimization problem. In Section III we use unitary transformations to simplify the problem, solve it exactly when $p = 2$, reduce the general case to the analysis of a single parameter, and report numerical work which supports the conclusion that the optimal inputs are independent of p . In Section IV, which can be skipped on first reading, we analyze the behavior of the output eigenvalues under certain small perturbations. Although this analysis does not yield a proof for $p \neq 2$, it does support our conjectures and yield a proof for $p = \infty$. In Section V we summarize our conclusions in the form of both conjectures and theorems, and summarize the evidence for the former. These can be reformulated as statements about the trumping relation [26, 27, 28, 29, 30] which plays an important role in entanglement catalysis.

In addition to the isomorphism $\mathbf{C}_4 \simeq \mathbf{C}_2 \otimes \mathbf{C}_2$, there is also an isomorphism between vectors in \mathbf{C}_4 and matrices in M_2 , and a straightforward way to make this correspondence using the Pauli matrices. We describe this in Appendix A. Although the results are straightforward and/or well-known, they play an important role and it is useful to describe them in a fixed notation.

II. CHANNEL DEFINITION AND PROPERTIES

Let Ψ_λ denote the qubit depolarizing channel [22]

$$\Psi_\lambda(\gamma) = (1 - \lambda) \frac{1}{d} I(\text{Tr } \gamma) + \lambda \gamma \quad (6)$$

with $\lambda \in [-\frac{1}{3}, 1]$. From this we generate a correlated two-qubit channel of the form (1) whose action is

$$\Phi_{\beta, \mu, \lambda}(R) = (1 - \mu)(\Psi_\lambda \otimes \Psi_\lambda)(R) + \mu (\text{Tr } R) |\beta\rangle\langle\beta|, \quad (7)$$

where $0 \leq \mu \leq 1$ and $|\beta\rangle$ is a fixed maximally entangled state of the two qubits. Although (7) is well-defined for any matrix in M_4 , we are interested in the case of density matrices, for which $R > 0$ and $\text{Tr } R = 1$. We will exploit the covariance property of the depolarizing channel, i.e.

$$\Psi_\lambda(U\rho U^\dagger) = U\Psi_\lambda(\rho)U^\dagger, \quad (8)$$

which holds for any unitary U matrix in M_2 . We find a relationship between the channel obtained using the Bell state $|\beta_0\rangle \equiv \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and any other maximally entangled state by observing

$$\begin{aligned} & \Phi_{\beta_0, \mu, \lambda}[(U \otimes V)R(U^\dagger \otimes V^\dagger)] \\ &= (U \otimes V)[(1 - \mu)(\Psi_\lambda \otimes \Psi_\lambda)(R) + \mu|\beta\rangle\langle\beta|](U^\dagger \otimes V^\dagger) \\ &= (U \otimes V)\Phi_{\beta, \mu, \lambda}(R)(U^\dagger \otimes V^\dagger) \end{aligned} \quad (9)$$

where

$$|\beta\rangle = (U^\dagger \otimes V^\dagger)|\beta_0\rangle = (I \otimes V^\dagger \overline{U})|\beta_0\rangle \quad (10)$$

and the second equality used (A3). Since unitary transformations do not affect eigenvalues,

$$\|\Phi_{\beta_0, \mu, \lambda}[(U \otimes V)R(U^\dagger \otimes V^\dagger)]\|_p = \|\Phi_{\beta, \mu, \lambda}(R)\|_p. \quad (11)$$

when $|\beta\rangle$ is given by (10). Because the p -norm is convex, it suffices to consider the optimization (4) for pure states $R = |\psi\rangle\langle\psi|$.

We now define an equivalence relation on pure states $|\psi\rangle \in \mathbf{C}^4$ by

$$|\psi_1\rangle \cong |\psi_2\rangle \Leftrightarrow \exists \text{ unitary } U, V : U \otimes V|\psi_1\rangle = |\psi_2\rangle. \quad (12)$$

Since all members of a given equivalence class are related by local unitaries, they have the same entanglement. In the matrix picture described in Appendix A, each equivalence class is characterized by its singular values. Moreover, we can characterize each equivalence class by its entanglement as measured by the entropy of its reduced density matrix (or by replacing h in (A8) by another function strictly monotone on $[0, 1]$). In particular, we find it useful to use the so-called ‘‘linear entropy’’ $E = 2(1 - \text{Tr } \gamma^2)$ in numerical work.

We now let $|\widehat{\psi}\rangle$ denote an equivalence class or, more properly, a representative of the class with properties to be specified in the next section. Then it follows from (11) that

$$\begin{aligned} & \sup_{\psi} \|\Phi_{\beta_0, \mu, \lambda}(|\psi\rangle\langle\psi|)\|_p \\ &= \sup_{\widehat{\psi}} \sup_{U, V} \|\Phi_{\beta_0, \mu, \lambda}[(U \otimes V)|\widehat{\psi}\rangle\langle\widehat{\psi}|(U^\dagger \otimes V^\dagger)]\|_p \\ &= \sup_{\widehat{\psi}} \sup_{\beta} \|\Phi_{\beta, \mu, \lambda}(|\widehat{\psi}\rangle\langle\widehat{\psi}|)\|_p \end{aligned} \quad (13)$$

with $|\beta\rangle$ maximally entangled.

The observations above allow us to draw several conclusions

a) First, (11) implies that $|\psi\rangle$ is an optimal input for $\Phi_{\beta, \mu, \lambda}$ if and only if $U \otimes V|\psi\rangle$ is an optimal input for $\Phi_{\beta_0, \mu, \lambda}$. Therefore,

$$\nu_p(\Phi_{\beta, \mu, \lambda}) = \nu_p(\Phi_{\beta_0, \mu, \lambda}), \quad (14)$$

The same conclusion can be reached by reversing the roles of $|\beta_0\rangle$ and $|\beta\rangle$ in (13). Thus, it is sufficient to study $\Phi_{\beta_0, \mu, \lambda}$.

b) If the optimal $|\widehat{\psi}\rangle$ in the reformulation (13) is unique, then the set of optimal inputs for $\Phi_{\beta_0, \mu, \lambda}$ is a subset of $\{|\psi\rangle = (U^\dagger \otimes V^\dagger)|\widehat{\psi}\rangle : U, V \text{ unitary}\}$. Thus, we expect that, excluding some trivial cases ($\lambda = 0$ or $\mu = 1$), all optimal inputs for a given channel have the same entanglement.

c) The singlet state $|\beta_2\rangle = \sigma_2|\beta_0\rangle$ satisfies the covariance condition $U \otimes U|\beta_2\rangle = |\beta_2\rangle$ for all unitary $U \in M_2$. Therefore, if we modify the equivalence relation (12) by restricting to $U = V$,

$$\nu_p(\Phi_{\beta_2, \mu, \lambda}) = \sup_{\tilde{\psi}} \|\Phi_{\beta_2, \mu, \lambda}(|\tilde{\psi}\rangle\langle\tilde{\psi}|)\|_p \quad (15)$$

where $|\tilde{\psi}\rangle$ denotes a representative of the modified equivalence class.

Before performing the optimization, we mention some trivial cases, always using the channel with $|\beta_0\rangle$ for the shift. When $\lambda = 0$ or $\mu = 1$, all inputs have the same output, namely $\frac{1}{4}(1-\mu)I + \mu|\beta_0\rangle\langle\beta_0|$. We will see that these are the only cases in which inputs with different entanglement are optimal. When $\mu = 1$, the optimal input $|\beta_0\rangle$ is unique and the optimal output is also $|\beta_0\rangle$. Henceforth, we will assume that $\lambda \in (0, 1)$ and $\mu \in [0, 1)$. When $\mu = 0$ every product state is an optimal input; at the end of Section III D we prove that, as expected, all other states are non-optimal.

III. OPTIMIZATION

A. Simplifying the input

After taking into account the normalization condition and irrelevance of an overall phase factor, the optimization problem for $\nu_p(\Phi_{\beta_0, \mu, \lambda})$ involves three complex, or six real, variables. The covariance used to obtain (13) reduces this to four real variables, one for $\hat{\psi}$ and three for $|\beta\rangle$. Moreover, the additional symmetry noted in (c) above allows an immediate reduction to three real variables. We use a different approach; the reduction from four to three real variables is obtained following (22). In

Section III D, we find that it would suffice to analyze the dependence on a single variable with the others fixed.

Using the notation of Appendix A for the maximally entangled Bell states, we can write an arbitrary state $\psi \in \mathbf{C}_4$ as

$$|\psi\rangle = \sum_k a_k |\beta_k\rangle = \sum_k a_k (I \otimes \sigma_k) |\beta_0\rangle = (I \otimes A) |\beta_0\rangle, \quad (16)$$

where $A = \sum_k a_k \sigma_k \in M_2$. Moreover, we can use the SVD to choose unitary matrices U, V so that $(U \otimes V)|\psi\rangle = (I \otimes V A U^T)|\beta_0\rangle$ with $V A U^T$ diagonal and positive, as discussed in Appendix A. It will be convenient to write the corresponding state (A5) using an angular variable $\theta \in [0, \frac{\pi}{2}]$ so that

$$(U \otimes V)|\psi\rangle = |\psi_\theta\rangle \equiv \frac{1}{\sqrt{2}}(\cos \frac{\theta}{2} + \sin \frac{\theta}{2})|\beta_0\rangle + \frac{1}{\sqrt{2}}(\cos \frac{\theta}{2} - \sin \frac{\theta}{2})|\beta_3\rangle, \quad (17)$$

which implies

$$|\psi_\theta\rangle\langle\psi_\theta| = \frac{1}{2} \left[I \otimes I + \sigma_z \otimes \sigma_z + \cos \theta (\sigma_z \otimes I + I \otimes \sigma_z) + \sin \theta (\sigma_x \otimes \sigma_x - \sigma_y \otimes \sigma_y) \right]. \quad (18)$$

B. Computing $\|\Phi_{\beta, \mu, \lambda}(|\psi_\theta\rangle\langle\psi_\theta|)\|_p$

Since $\Psi_\lambda(\sigma_k) = \lambda \sigma_k$ it is straightforward to see that (18) implies

$$\begin{aligned} & (\Psi_\lambda \otimes \Psi_\lambda)(|\psi_\theta\rangle\langle\psi_\theta|) \\ &= \frac{1}{4} \left[I \otimes I + \lambda^2 \sigma_z \otimes \sigma_z + \cos \theta \lambda (\sigma_z \otimes I + I \otimes \sigma_z) + \sin \theta \lambda^2 (\sigma_x \otimes \sigma_x - \sigma_y \otimes \sigma_y) \right], \end{aligned} \quad (19)$$

which can be written as

$$(\Psi_\lambda \otimes \Psi_\lambda)(|\psi_\theta\rangle\langle\psi_\theta|) = \frac{1}{4} \begin{pmatrix} 1 + \lambda^2 + 2\lambda \cos \theta & 0 & 0 & 2\lambda^2 \sin \theta \\ 0 & (1 - \lambda^2) & 0 & 0 \\ 0 & 0 & (1 - \lambda^2) & 0 \\ 2\lambda^2 \sin \theta & 0 & 0 & 1 + \lambda^2 - 2\lambda \cos \theta \end{pmatrix}. \quad (20)$$

Now writing $V^\dagger \overline{U} = \begin{pmatrix} a & \bar{b} \\ -b & \bar{a} \end{pmatrix}$ with $|a|^2 + |b|^2 = 1$, we find

$$\langle \beta | = \langle \beta_0 | (V^\dagger \overline{U})^\dagger = \langle \beta_0 | \begin{pmatrix} \bar{a} & -\bar{b} \\ b & a \end{pmatrix} = (\bar{a} \ -\bar{b} \ b \ a). \quad (21)$$

Using (20) and (21) we find that $\Phi_{\beta, \mu, \lambda}(|\psi_\theta\rangle\langle\psi_\theta|)$ is given by

$$\frac{1-\mu}{4} \begin{pmatrix} 1 + \lambda^2 + 2\lambda \cos \theta & 0 & 0 & 2\lambda^2 \sin \theta \\ 0 & 1 - \lambda^2 & 0 & 0 \\ 0 & 0 & 1 - \lambda^2 & 0 \\ 2\lambda^2 \sin \theta & 0 & 0 & 1 + \lambda^2 - 2\lambda \cos \theta \end{pmatrix} + \frac{\mu}{2} \begin{pmatrix} |a|^2 & -a\bar{b} & ab & a^2 \\ -\bar{a}b & |b|^2 & -b^2 & -ab \\ \bar{a}b & -\bar{b}^2 & |b|^2 & ab \\ \bar{a}^2 & -\bar{a}b & \bar{a}b & |a|^2 \end{pmatrix}.$$

It is evident that $(0 \ b \ \bar{b} \ 0)^T$ is an eigenvector of both matrices above. This suggests that we make a simplification exploiting the block structure in the left matrix using a basis which includes the known eigenvector. We act first on both matrices with the permutation matrix P which exchanges the 2nd and 4th rows and columns, and then make a unitary transformation which preserves the block structure and achieves a partial diagonalization. Thus, we replace each matrix above by $W^\dagger P(\)PW$ where

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad W = \frac{1}{\sqrt{2}} \begin{pmatrix} \frac{1}{|a|} \begin{pmatrix} a & a \\ \bar{a} & -\bar{a} \end{pmatrix} & 0 \\ 0 & \frac{1}{|b|} \begin{pmatrix} \bar{b} & \bar{b} \\ b & -b \end{pmatrix} \end{pmatrix}. \quad (22)$$

Although these unitary transformations do *not* preserve entanglement, they do not affect the eigenvalues of the output. After introducing the shorthand $c_\varphi \equiv \cos \varphi$, $s_\varphi \equiv \sin \varphi$, $S = 2\lambda \sin \theta$, $C = 2\lambda \cos \theta$, and $M_\mu = 4\mu/(1-\mu)$, we find that the transformed output density matrix is

$$\frac{1-\mu}{4} \begin{pmatrix} 1+\lambda^2 + c_\varphi \lambda S + M_\mu |a|^2 & C + i s_\varphi \lambda S & 0 & M_\mu \sqrt{|a|^2(1-|a|^2)} \\ C - i s_\varphi \lambda S & 1 + \lambda^2 - c_\varphi \lambda S & 0 & 0 \\ 0 & 0 & 1-\lambda^2 & 0 \\ M_\mu \sqrt{|a|^2(1-|a|^2)} & 0 & 0 & 1-\lambda^2 + M_\mu(1-|a|^2) \end{pmatrix}. \quad (23)$$

We have now reduced the optimization to a problem in three real variables, $\sin \theta, \varphi, |a|$.

C. Optimization for $p = 2$

It follows from (23) and some elementary algebra that

$$\begin{aligned} & \|\Phi_{\beta, \mu, \lambda}(|\psi_\theta\rangle\langle\psi_\theta|)\|_2^2 \\ &= (\frac{1-\mu}{4})^2 \left\{ M_\mu^2 + 2M_\mu [2\lambda^2|a|^2 + (1-\lambda^2) + c_\varphi \lambda S] \right. \\ & \quad \left. + 4(1+\lambda^2)^2 - 2S^2(1-\lambda^2) \right\} \end{aligned} \quad (24)$$

Since only the coefficient of M_μ includes any dependence on a and $M_\mu > 0$, it follows that the 2-norm is largest when this coefficient is largest (see Fig. 1). This occurs when $|a| = 1$, and $c_\varphi = 1$. After making these choices we find

$$\begin{aligned} & \|\ \|^2_2 = (\frac{1-\mu}{4})^2 [M_\mu^2 + 2M_\mu(1+\lambda^2 + \lambda S) \\ & \quad + 4(1+\lambda^4) + 2(C^2 + \lambda^2 S^2)] \\ &= (\frac{1-\mu}{4})^2 [M_\mu^2 + 2M_\mu(1+\lambda^2 + 2\lambda^2 \sin \theta) \\ & \quad + 4(1+\lambda^2)^2 - 4\lambda^2(1-\lambda^2) \sin^2 \theta] \end{aligned} \quad (25)$$

which can be regarded as a quadratic function of $\sin \theta$ whose optimization is straightforward. Since we obtain an equivalent problem whenever the optimum is achieved with $|a| = 1$, we give the details in the next section.

D. Consequences of $|a| = 1$ optimal

We now describe the conclusions one can reach if the optimal output p -norm is achieved when $|a| = 1$. We will

show that when this is the case, the optimal inputs are the same as for $p = 2$.

When $|a| = 1$, the output density matrix (23) is block diagonal. Two of its eigenvalues are $\frac{1}{4}(1-\mu)(1-\lambda^2)$ and the remaining two are

$$\begin{aligned} & \frac{1}{4}(1-\mu)(1-\lambda^2) + \frac{1}{2}\mu \\ & \pm \frac{1}{4}(1-\mu)\sqrt{\frac{1}{4}M_\mu^2 + 4\lambda^2 - (1-\lambda^2)S^2 + M_\mu c_\varphi \lambda S}. \end{aligned} \quad (26)$$

The output p -norm will be largest, and output entropy smallest, when the quantity under the square root is largest. Therefore, one should choose $c_\varphi = 1$. This implies that $V^\dagger \bar{U} = I$ or, equivalently, that $V = \bar{U}$.

The optimization problems for both (25) and (26) then reduce to maximizing a function of the form

$$-4(1-\lambda^2)\lambda^2 \sin^2 \theta + 2\lambda^2 M_\mu \sin \theta + \text{constant} \quad (27)$$

which is quadratic in $\sin \theta > 0$ when $\lambda \in (0, 1)$. This is largest when $\sin \theta = \min\{1, \frac{\mu}{1-\mu}, \frac{1}{1-\lambda^2}\}$. We distinguish two situations characterized by the threshold value $\mu_c \equiv \frac{1-\lambda^2}{2-\lambda^2}$ corresponding to the boundary $\sin \theta = 1$.

- **Below Threshold:** If $\mu < \mu_c$ then the maximum value of (27) is achieved for $4\sin \theta(1-\lambda^2) = M_\mu = 4\frac{\mu}{1-\mu}$, or, equivalently

$$\theta = \sin^{-1} \left[\frac{\mu}{1-\mu} \frac{1}{1-\lambda^2} \right] = \sin^{-1} \left[\frac{\mu(1-\mu_c)}{\mu_c(1-\mu)} \right]. \quad (28)$$

Moreover, since $V = \bar{U}$, the optimum is achieved with a family of input states of the form

$$|\psi_{\text{opt}}\rangle = (V^T \otimes V^\dagger) |\psi_\theta\rangle, \quad (29)$$

with θ as in (28), $|\psi_\theta\rangle$ as in (17), and V an arbitrary unitary. Using (A7), one finds that the reduced

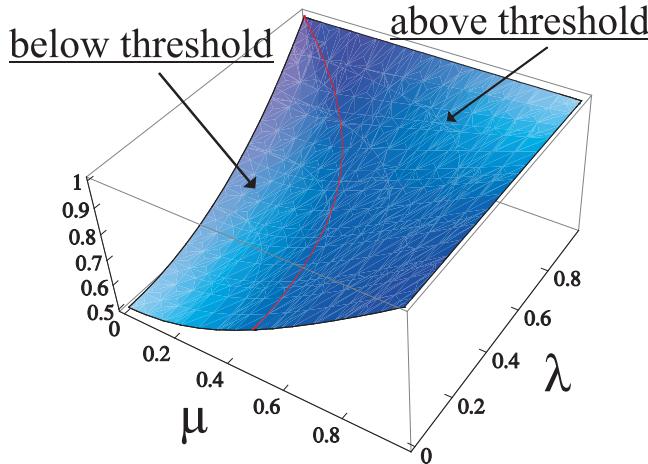


FIG. 1: Plot of the 2-norm for the channel $\Phi_{\beta_0, \mu, \lambda}$. The continuous curve represents the threshold boundary. For $\mu = 1$ or $\lambda = 1$ the norm is 1: in the former case the channel sends every input state into $|\beta_0\rangle\langle\beta_0|$; in the latter, it transforms the input $|\psi\rangle\langle\psi|$ into a mixture of $|\psi\rangle\langle\psi|$ and $|\beta_0\rangle\langle\beta_0|$ so that choosing $|\psi\rangle = |\beta_0\rangle$ gives a pure output.

density matrix of $|\psi_\theta\rangle$ is

$$\gamma_\theta = \frac{1}{2}[I + \cos \theta \sigma_3] \quad (30)$$

and the entanglement of any optimal input is simply $h(\cos \theta)$ where h is the binary entropy (A8), or $E = \sin^2 \theta$ when the linear entropy is used (see Fig. 2).

- **At or above Threshold:** For $\mu \geq \mu_c$ the maximum value of (27) is achieved for $\sin \theta = 1$. Then (17) gives $|\psi_\theta\rangle = |\beta_0\rangle$ and the diagonal matrix D_θ is simply the identity so that $V^\dagger D_\theta V = V^\dagger V = I$. Thus, there is a single optimal input, the maximally entangled state $|\beta_0\rangle$.

Note that for $\mu = 0$ the value of $|a|$ is irrelevant and the optimization gives a special case of (27) with the optimum achieved for $\theta = 0$, consistent with (28). Because there is no dependence on a in this case, this result holds for all p and for all $|\beta\rangle$ in (13). Hence, $V^\dagger \overline{U}$ is arbitrary and we recover the expected result that all product inputs are optimal. Because $\theta \neq 0$ can never yield a state in the equivalence class with no entanglement, we also find that a state which is not a product can not be optimal.

E. Numerical results

It is not easy to perform an exact analytical analysis of the output p -norms for $p \neq 2$. However extensive numerical studies of optimization were carried out using the equivalent Renyi entropy [25], for over 2000 pairs of randomly chosen value of μ and λ . In all cases, we found that the input states which are optimal for $p = 2$ are

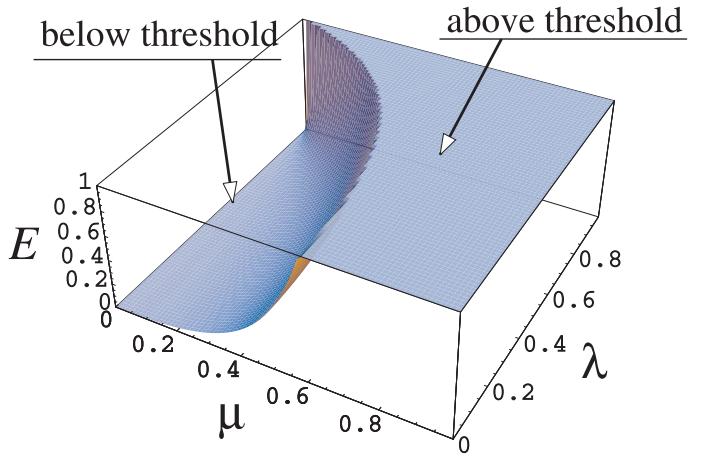


FIG. 2: Entanglement of the optimal input states which maximize the 2-norm for the map $\Phi_{\beta_0, \mu, \lambda}$. For $\mu \in [0, \mu_c]$ the entanglement of the optimal inputs is a strictly monotone function of μ ; for $\mu \geq \mu_c$ the optimal input is the maximally entangled state $|\beta_0\rangle$.

also optimal for $p > 1$. In Fig. 3, we show typical numerical results of our findings by comparing the minimal Rényi output entropies (5) for randomly chosen inputs with that of optimal inputs for $p = 2$, which lie on the bottom curve. In all cases the output Renyi entropy was larger than the expected minimum.

IV. PARTIAL ANALYSIS WITH HEURISTICS

A. Eigenvalue behavior from characteristic polynomial

In this section, we attempt to show that the optimal p -norm is attained when $|a| = 1$ by showing that it increases monotonically with $|a|$. Although our argument is incomplete and can not exclude fluctuations under some conditions, it does provide additional support for this conjecture. To analyze the behavior of the eigenvalues of (23) as a function of the parameters $|a|$ and φ , we use the characteristic polynomial of the output density matrix to estimate the effect of small changes after reduction to a 3-dimensional problem.

Since $\frac{1}{4}(1 - \mu)(1 - \lambda^2)$ is clearly an eigenvalue of (23), we are left with the eigenvalue problem for the 3×3 matrix

$$\Delta = (1 + \lambda^2)I + \begin{pmatrix} c_\varphi \lambda S + M_\mu |a|^2 & C + i s_\varphi \lambda S & M_\mu \sqrt{|a|^2(1 - |a|^2)} \\ C - i s_\varphi \lambda S & -c_\varphi \lambda S & 0 \\ M_\mu \sqrt{|a|^2(1 - |a|^2)} & 0 & -2\lambda^2 + M(1 - |a|^2) \end{pmatrix} \quad (31)$$

where C, S, φ and M_μ are defined as in (23).

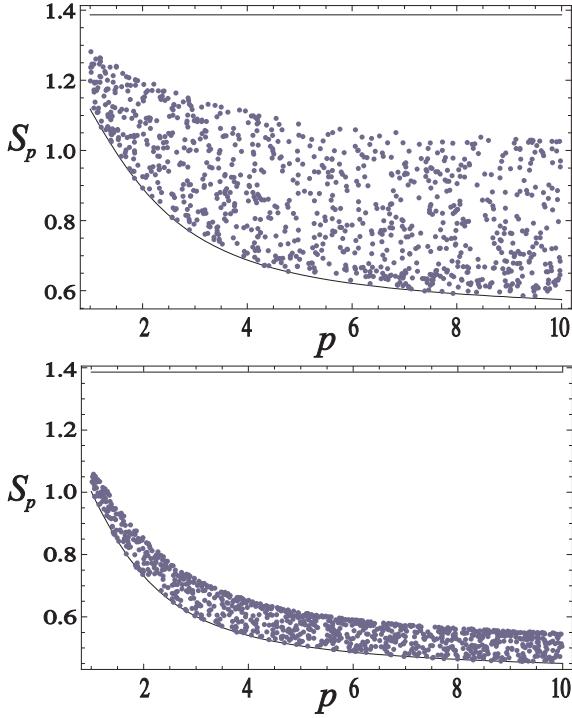


FIG. 3: Scatter plots of the output Renyi entropy $S_p[\Phi_{\beta_0, \mu, \lambda}(|\psi\rangle\langle\psi|)]$ as a function of p for randomly chosen inputs compared to that for the conjectured optimal input. The horizontal line corresponds to the maximum possible Renyi entropy of $\ln 4$. Top: $\lambda = \frac{1}{2}, \mu = \frac{1}{4} < \mu_c = \frac{3}{7}$ below threshold. Bottom: $\lambda = \frac{1}{3}, \mu = \frac{1}{2} > \mu_c = \frac{8}{17}$ above threshold.

The characteristic polynomial for $\Delta - (1 + \lambda^2)I$ is

$$\begin{aligned} \hat{R}(\zeta) = & -\zeta^3 + (M_\mu - 2\lambda^2)\zeta^2 + [C^2 + \lambda^2 S^2 + M_\mu |a|^2(2\lambda^2 \\ & + c_\varphi \lambda S)]\zeta + (C^2 + \lambda^2 S^2)(2\lambda^2 - M) \\ & + M_\mu |a|^2(C^2 + \lambda^2 S^2 + 2\lambda^3 c_\varphi S) \\ \equiv & R_0(\zeta) + M_\mu |a|^2(2\lambda^2 + c_\varphi \lambda S)\zeta \\ & + M_\mu |a|^2(C^2 + \lambda^2 S^2 + 2\lambda^3 c_\varphi S). \end{aligned} \quad (32)$$

This defines $R_0(\zeta)$. Then with $x = \zeta + 1 + \lambda^2$, the characteristic polynomial for Δ is

$$\begin{aligned} R(x) = & R_0(x - 1 - \lambda^2) + M_\mu |a|^2 \left[(2\lambda^2 + c_\varphi \lambda S)x \right. \\ & \left. + (1 - \lambda^2)(2\lambda^2 - c_\varphi \lambda S - S^2) \right], \end{aligned} \quad (33)$$

where we used $C^2 + S^2 = 4\lambda^2$.

B. Optimization for $1 < p < 2$

We first assume that a, S are fixed and consider the optimal value of $c_\varphi = \cos \varphi$ by examining the effect of the change $c_\varphi \mapsto c_\varphi + \epsilon$. We apply Lemma 6 with $P(x) = R(x)$ given by (33), and $\delta_1 = \epsilon M_\mu |a|^2 \lambda S$ and

$\delta_2 = -\epsilon M_\mu |a|^2 \lambda S(1 - \lambda^2)$ to find that the eigenvalues of Δ

$$v_k \mapsto v_k + \epsilon M_\mu |a|^2 \lambda S \frac{1}{(v_k - v_m)(v_k - v_n)} [v_k - (1 - \lambda^2)] \quad (34)$$

with k, m, n distinct. It then follows from Lemmas 7 and 8 using the expressions (B8) and (B10) that

$$\begin{aligned} \|\mathbf{v}\|^p \mapsto & \|\mathbf{v}\|^p + \epsilon M_\mu |a|^2 \lambda S \frac{p}{v_1 - v_3} \left[p(\dot{v}_1^{p-1} - \dot{v}_3^{p-1}) \right. \\ & \left. - (p-1)(1 - \lambda^2)(\dot{v}_1^{p-2} - \dot{v}_3^{p-2}) \right] + O(\epsilon^2) \end{aligned} \quad (35)$$

where $v_1 > \dot{v}_1 > v_2 > \dot{v}_3 > v_3$ and similarly for \dot{v}_k . Then the quantity in square brackets $[\] > 0$ is positive for $1 < p < 2$. Since $\lambda S = 2\lambda^2 \sin \theta \geq 0$ (by our assumption $\theta \in [0, \frac{\pi}{2}]$), $\|\Delta\|_p^p$ increases as c_φ goes from -1 to $+1$ and is thus largest when $c_\varphi = 1$.

To study the effect of changing $|a|$, first observe that when $c_\varphi = 1$, $2\lambda^2 - c_\varphi \lambda S - S^2 = 2\lambda^2(1 + \sin \theta)(1 - 2\sin \theta)$. If we insert this in (33), we can apply Lemma 6 with $P(x) = R(x)$, $\delta_1 = \epsilon 2\lambda^2 M_\mu (1 + \sin \theta)$ and $\delta_2 = \epsilon 2\lambda^2 M_\mu (1 + \sin \theta)(1 - \lambda^2)(1 - 2\sin \theta)$ to conclude that

$$\begin{aligned} v_k \mapsto & v_k + \epsilon 2\lambda^2 M_\mu (1 + \sin \theta) \frac{1}{(v_k - v_m)(v_k - v_n)} [v_k \\ & + (1 - \lambda^2)(1 - 2\sin \theta)] \end{aligned} \quad (36)$$

We again apply Lemmas 7 and 8 using the expressions (B8) and (B10) to conclude that

$$\begin{aligned} \|\mathbf{v}\|^p \mapsto & \|\mathbf{v}\|^p + \epsilon B \left[p(\dot{v}_1^{p-1} - \dot{v}_3^{p-1}) + (p-1)(1 - \lambda^2) \right. \\ & \left. (1 - 2\sin \theta)(\dot{v}_1^{p-2} - \dot{v}_3^{p-2}) \right] + O(\epsilon^2) \end{aligned} \quad (37)$$

with \dot{v}_k, \dot{v}_k constrained as above and $B = 2\lambda^2 M_\mu (1 + \sin \theta) \frac{p}{v_1 - v_3} > 0$. However, $\dot{v}_1^{p-2} < \dot{v}_3^{p-2}$ because $p - 2 < 0$. Therefore, we can only conclude that the quantity in brackets is positive when $\sin \theta \geq \frac{1}{2}$. Otherwise, (35) has two competing positive and negative terms.

When $\mu > \frac{1 - \lambda^2}{3 - \lambda^2}$, the optimum in (28) satisfies $\sin \theta > \frac{1}{2}$. Even if the p -norm does not increase monotonically with $|a|$ for small values of θ , it seems likely that the optimum is still achieved when $|a| = 1$.

C. Optimization for $p > 2$

When $p > 2$, the expression (35) contains competing terms and we cannot reach a definite conclusion about the effect of $c_\varphi \mapsto c_\varphi + \epsilon$. However, both (34) and (36) still imply that the largest eigenvalue increases under the changes $c_\varphi \mapsto c_\varphi + \epsilon$ and $|a|^2 \mapsto |a|^2 + \epsilon$ with $\epsilon > 0$. Moreover, if one fixes φ and considers the change $|a|^2 \mapsto |a|^2 + (\delta_1 x + \delta_2)$ with

$$\delta_1 = \epsilon 2 M_\mu \lambda^2 (1 + c_\varphi \sin \theta) x \quad (38)$$

$$\delta_2 = \epsilon 2 M_\mu \lambda^2 (1 - \lambda^2) (1 - c_\varphi \sin \theta - 2 \sin^2 \theta) \quad (39)$$

then Lemmas 6 and 7 imply that

$$\begin{aligned} \|\Delta\|_p^p &\mapsto \|\Delta\|_p^p + \epsilon B p (1 + c_\varphi \sin \theta) (\hat{v}_1^{p-1} - \hat{v}_3^{p-1}) \\ &\quad + \epsilon B (p-1) (1 - \lambda^2) (1 - c_\varphi \sin \theta) \\ &\quad - 2 \sin^2 \theta (\hat{v}_1^{p-2} - \hat{v}_3^{p-2}) + O(\epsilon^2) \end{aligned} \quad (40)$$

where $B = 2\lambda^2 M_\mu p$. When $\sin \theta < \frac{1}{2}$ this implies that $\|\Delta\|_p$ increases with $|a|^2$. This is sufficient to show that when $\mu < \frac{1-\lambda^2}{3-\lambda^2}$ at least a local optimum is achieved when $c_\varphi = 1$ and θ is given by (28).

D. Additional heuristics

One can apply the MVT again to (37) using \hat{v}_2, \hat{v}_3 to denote the mean values. Under the assumptions $\hat{v}_k \approx \hat{v}_k$ and $\hat{v}_2 \geq (1 - \lambda^2)$ the term in square brackets [] in (37) is

$$\approx (p-1) \frac{\hat{v}_1 - \hat{v}_3}{\hat{v}_2^2} (1 - \lambda^2) 2 [(p-1)(1 - \sin \theta) + \sin \theta] \geq 0 \quad (41)$$

when $1 < p < 2$. For $p > 2$, a similar analysis beginning from (40) gives a change in $\|\Delta\|_p^p$ approximately proportional to

$$(p-2)(1 - \sin^2 \theta) + (1 + c_\varphi \sin \theta) \geq 0. \quad (42)$$

This approach can even be applied to the entropy to show that when $|a|$ increases the output entropy decreases under the assumptions above. We omit the details.

Since $v_1 > \hat{v}_1 > \hat{v}_2 > \hat{v}_3 > v_3$, one knows that \hat{v}_2 is larger than the smallest eigenvalue of Δ and probably close to the second largest, which one expects to be $> 1 - \lambda^2$. Thus, the assumptions above are reasonable. However, this is far from the desired proof that the output p -norm increases with $|a|$ and is thus optimal for $|a| = 1$. For $p > 2$, these heuristics are more convincing because errors from these approximations are better controlled.

V. CONCLUSIONS

A. Main results

Conjecture 1 Let $\Phi_{\beta_0, \mu, \lambda}$ be a channel on M_4 as defined in (7) with $\mu, \lambda \in (0, 1)$ and let $\mu_c = \frac{1-\lambda^2}{2-\lambda^2}$. Then

i) For $0 < \mu < \mu_c$ the maximal output p -norm is achieved with a family of input states of the form $V^T \otimes V |\psi_\theta\rangle$ with V unitary and $|\psi_\theta\rangle$ given by (16) with $\theta = \sin^{-1}(\frac{\mu}{1-\mu} \frac{1}{1-\lambda^2}) \in (0, \frac{\pi}{2})$.

ii) For $\mu \geq \mu_c$ the optimal output 2-norm is achieved if and only if the input is the maximally entangled state $|\beta_0\rangle$.

Moreover, the same conclusions hold for the minimal output entropy.

In Section III C this conjecture was proved for $p = 2$. Since $\|\gamma\|_\infty$ is simply the largest eigenvalue of γ , the observations at the start of Section IV C, imply that the optimal input is achieved for $a = 1$ when $p = \infty$. The conjecture then follows from the results in Section III D.

Theorem 2 Conjecture 1 holds for $p = 2$ and for $p = \infty$.

Conjecture 1 is supported by extensive numerical work, as discussed in Section III E. Additional evidence for the conjecture can be summarized as follows.

- a) When $1 < p < 2$ and $\mu > \frac{1-\lambda^2}{3-\lambda^2}$ either Theorem 1 holds or the optimal input is achieved with a state of the form $U \otimes V |\psi_\theta\rangle$ with $U \neq V^T$ and $0 < \theta < \sin^{-1} \frac{1}{2}$. The latter would be unexpected, but has not been excluded.
- b) When $p > 2$ and $\mu < \frac{1-\lambda^2}{3-\lambda^2}$ either Theorem 1 holds or the optimal input is achieved with a state of the form $U \otimes V |\psi_\theta\rangle$ with $U \neq V^T$ and $\theta > \sin^{-1} \frac{1}{2}$. Again, this seems unlikely.
- c) The heuristic argument described in Section IV D makes other behavior unlikely, especially for $p > 2$.
- d) For $1 < p < 2$, Corollary 4 below excludes the possibility that the optimal input is maximally entangled for $\mu < \mu_c$.

The conjectured behavior is very different from that for the shifted depolarizing channel on M_4 which maps

$$R \mapsto (1 - \mu) [\lambda R + (1 - \lambda) (\text{Tr } R) \frac{1}{4} I_4] + \mu (\text{Tr } R) |\beta\rangle \langle \beta| \quad (43)$$

where $|\beta\rangle$ is fixed and the quantity in square brackets [] is easily recognized as the usual depolarizing channel on M_4 . In this case the optimal input is always achieved using the vector $|\beta\rangle$ which defines the shift. Changing from the usual depolarizing channel on M_4 to a product of qubit channels $\Psi_\lambda \otimes \Psi_\lambda$ dramatically changes the effect of the correlation introduced by a maximally entangled shift $|\beta\rangle$ for values of $\mu < \mu_c$.

Even without proving the conjecture, the next theorem implies that for $1 < p \leq 2$ and for the minimal output entropy, the optimal input is never achieved with a maximally entangled state when $\mu < \mu_c$. Moreover, to extend this result to $p > 2$, it would suffice to show that the optimal output is achieved with $c_\varphi = 1$.

Theorem 3 For $1 < p \leq 2$, the maximal output p -norm of the channel $\Phi_{\beta_0, \mu, \lambda}$ defined in (7) is achieved with a maximally entangled input if and only if that input is $|\beta_0\rangle$. The same result holds for the minimal output entropy.

Proof: for $1 < p \leq 2$ the optimal output is achieved with $c_\varphi = 1$. For any p the optimal input is maximally

entangled if and only if $\theta = \frac{\pi}{2}$ in (17). Then $\sin \theta = 1$ and (31) implies

$$\begin{aligned} & \Delta - (1 + \lambda^2)I \\ &= \begin{pmatrix} +M_\mu|a|^2 & 0 & M_\mu\sqrt{|a|^2(1-|a|^2)} \\ 0 & -2\lambda^2 & 0 \\ M_\mu\sqrt{|a|^2(1-|a|^2)} & 0 & -2\lambda^2 + M(1-|a|^2) \end{pmatrix} \end{aligned} \quad (44)$$

from which it follows immediately that one eigenvalue of Δ is $1 + \lambda^2 - 2\lambda^2 = 1 - \lambda^2$ and the other two are

$$1 + \lambda^2 + \frac{1}{2}M_\mu \pm \sqrt{\frac{1}{4}M_\mu^2 + 4\lambda^4 - 2\lambda^2M_\mu(1-2|a|^2)} \quad (45)$$

which gives the largest p -norm when the term under the square root is largest, i.e., when $|a|^2 = 1$. But then, the results of Section III D apply. **QED**

Corollary 4 For $1 < p < 2$ and $\mu < \mu_c$ the optimal output of the channel $\Phi_{\beta_0, \mu, \lambda}$ is never attained with a maximally entangled input. The same result holds for the minimal output entropy.

B. Majorization and trumping

Let $|\psi_{\text{opt}}\rangle$ be the canonical vector $|\psi_\theta\rangle$ for the family of input states which achieves the optimal 2-norm output for $\Phi_{\beta_0, \lambda, \mu}$, or, equivalently a state of the form $V \otimes V^T |\psi_\theta\rangle$ as described in part (i) of Conjecture 1. If true, this conjecture would imply that for any $p > 1$, the output p -norms satisfy

$$\|\Phi_{\beta_0, \lambda, \mu}(|\psi_{\text{opt}}\rangle\langle\psi_{\text{opt}}|)\|_p \geq \|\Phi_{\beta_0, \lambda, \mu}(|\psi\rangle\langle\psi|)\|_p \quad (46)$$

for any other input state $|\psi\rangle$. One might, therefore, expect that the eigenvalues of the matrix $\Phi_{\beta_0, \lambda, \mu}(|\psi_{\text{opt}}\rangle\langle\psi_{\text{opt}}|)$ majorize those of any other output. This is false, as can be seen from the following two examples.

First, let $\lambda = \frac{1}{3}$ and $\mu = \frac{1}{2}$. In this case $\mu > \mu_c = \frac{8}{17}$ so that the optimal input is $|\beta_0\rangle$, whose output eigenvalues are $\{0, 0.667, 0.111, 0.111, 0.111\}$. A numerical search found that the input product state of the form (A2) with $a_0 = a_2 = 0$ and $a_3 = \frac{1}{\sqrt{2}} = -ia_1$ yields an output state with eigenvalues $\{0.611, 0.222, 0.111, 0.056\}$ which is clearly not majorized by those of the preceding state. For an example with $\mu < \mu_c$, consider $\lambda = \frac{1}{2}$ and $\mu = \frac{1}{4}$. In this case the optimal input gives an output with eigenvalues $\{0.596, 0.141, 0.141, 0.123\}$. However, the same product state now yields an output with eigenvalues $\{0.422, 0.391, 0.141, 0.047\}$ which, again, are not majorized by those of the preceding state.

However, weak majorization $x \prec_w y$ (which does not require equal 1 norms) is well-known to be equivalent to the stronger condition that $\|x\| \leq \|y\|$ for all unitarily invariant norms [31, Corollary 3.5.9]. This is known as the Ky Fan dominance theorem [32]. Recently, Aubrun

and Nechita [29, 30] proved an analogous result for ℓ_p norms with $p \geq 1$ in which majorization is replaced by a relation known as “trumping”. This concept, introduced in connection with the phenomenon known as entanglement catalysis [28] plays an important role in quantum information theory. If there is a vector z such that $x \otimes z \prec y \otimes z$, then one says that the vector y trumps x and writes $x \prec_T y$. Moreover, it follows that $\|x\|_p \leq \|y\|_p$ for all $p > 1$. Aubrun and Nechita [29, 30] showed that $\|x\|_p \leq \|y\|_p$ for all $p > 1$ if and only if x is in the closure of the vectors trumped by y . Here, the closure is taken in the ℓ_1 norm and includes arbitrarily large catalyst vectors z . For a precise statement and other formulations, see [29, 30].

This leads us to the following reformulation of Conjecture 1

Conjecture 5 Let $\Phi_{\beta_0, \mu, \lambda}$ be a channel on M_4 as defined in (7) and let $\mu_c = \frac{1-\lambda^2}{2-\lambda^2}$.

i) For $0 < \mu < \mu_c$, let ψ_{opt} be as in (46). Then if $|\psi\rangle \neq (V^T \otimes V)|\psi_{\text{opt}}\rangle$ for some unitary V , the eigenvalues of $\Phi_{\beta_0, \lambda, \mu}(|\psi\rangle\langle\psi|)$ yield a vector in the closure of the set of vectors trumped by the eigenvalues of $\Phi_{\beta_0, \lambda, \mu}(|\psi_{\text{opt}}\rangle\langle\psi_{\text{opt}}|)$.

ii) For $\mu \geq \mu_c$ and any input $|\psi\rangle \neq |\beta_0\rangle$ the eigenvalues of $\Phi_{\beta_0, \lambda, \mu}(|\psi\rangle\langle\psi|)$ yield a vector in the closure of the set of vectors trumped by the eigenvalues of $\Phi_{\beta_0, \lambda, \mu}(|\beta_0\rangle\langle\beta_0|)$.

Conjecture 1 would follow immediately from Conjecture 5. It is, therefore, tempting to seek an analytic proof of this conjecture by seeking a catalyst z . Unfortunately, this is not easy in general. In our case, the fact that $(1-\mu)(1-\lambda^2)$ is always an output eigenvalue, allowed a reduction to an effective 3-dimensional problem. For $d = 3$, it is known [28] that trumping with a finite dimensional catalyst z is never possible, although examples are known [26, 27] which use a infinite-dimensional catalyst. Thus, although we believe Conjecture 5 holds, it seems more likely to be established by proving Conjecture 1 and then applying Aubrun and Nechita’s results [29, 30] than by finding a catalyst.

We can make additional reformulations suggested by the arguments in Section IV. For example, let Δ be given by (31) with $\mu, \lambda, \theta, \varphi$ fixed, and let $\mathbf{v}(|a|)$ denote its eigenvalues. Then if $\mathbf{v}(|a|) \prec_T \mathbf{v}(|1|)$ we could conclude that the optimal p -norm of $\Phi_{\beta_0, \mu, \lambda}$ is attained when $|a| = 1$. The validity of Conjecture 1 would then follow from the arguments in Section III D.

Acknowledgment It is a pleasure to recall that this work began when MBR and VG were visiting the Quantum Information Theory Group at the University of Pavia. The authors VG, CM and MBR also benefitted from discussions during workshops in Benasque and at the ICTP in Trieste. The contribution of MBR was partially supported by the National Science Foundation under Grants DMS-0314228 and DMS-0604900, and by the National Security Agency and Advanced Research and

Development Activity under Army Research Office contract number DAAD19-02-1-0065. The contribution of FC and VG has been in part supported by the Centro di Ricerca Ennio De Giorgi of the Scuola Normale Superiore.

APPENDIX A: ENTANGLEMENT PARAMETRIZATION

Let $|\beta_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and define $|\beta_k\rangle = (I \otimes \sigma_k)|\beta_0\rangle$ for $k = 1, 2, 3$ and σ_k denotes the Pauli matrices. These four orthogonal maximally entangled states form an orthonormal basis for \mathbf{C}^4 . The property $\text{Tr}_1|\beta_k\rangle\langle\beta_m| = \frac{1}{2}\sigma_k\sigma_m$, facilitates computation of reduced density matrices and entanglement of pure states represented in this basis. Our notation differs by a factor of i from the so-called “magic basis” introduced in [33].

When σ_k acts on the first qubit,

$$(\sigma_k \otimes I)|\beta_0\rangle = \begin{cases} |\beta_k\rangle & k = 1, 3 \\ -|\beta_2\rangle & k = 2 \end{cases} \quad (\text{A1})$$

An arbitrary pure state $|\psi\rangle \in \mathbf{C}_4$ can be written in the form

$$|\psi\rangle = \sum_{k=0}^3 a_k |\beta_k\rangle = (I \otimes A)|\beta_0\rangle \quad (\text{A2})$$

where $A = \sum_k a_k \sigma_k$ is in M_2 . This gives an isomorphism between vectors in \mathbf{C}_4 and matrices in M_2 . We henceforth restrict ourselves to normalized vectors for which $\|\psi\|^2 = \sum_{k=0}^3 |a_k|^2 = 1 = \frac{1}{2}\text{Tr} A^\dagger A$. Combining (A1) with the observation that $a_2 \mapsto -a_2$ takes $A \mapsto A^T$, we recover the well-known result that

$$|\psi\rangle = (I \otimes A)|\beta_0\rangle = (A^T \otimes I)|\beta_0\rangle \quad (\text{A3})$$

Since local unitary transformations do not affect the entanglement of $|\psi\rangle$, the state in (A2) has the same entanglement as any state of the form

$$\begin{aligned} (U \otimes V)|\psi\rangle &= \sum_k a_k (U \otimes I)(I \otimes V)(I \otimes \sigma_k)|\beta_0\rangle \\ &= (I \otimes V) \sum_k a_k (I \otimes \sigma_k)(I \otimes U^T)|\beta_0\rangle \\ &= (I \otimes V A U^T)|\beta_0\rangle. \end{aligned} \quad (\text{A4})$$

Moreover, by the singular value decomposition (SVD), one can choose U, V so that $V A U^T$ is diagonal and positive, i.e., $V A U^T = D = a_0 I + a_3 \sigma_3 \geq 0$. By including a suitable permutation in U, V one can further require that the singular values are in decreasing order, which is equivalent to $a_0 \geq a_3 \geq 0$. Thus, we can choose U, V unitary so that

$$|\widehat{\psi}\rangle = (U \otimes V)|\psi\rangle = (I \otimes V A U^T) = a_0 |\beta_0\rangle + a_3 |\beta_3\rangle \quad (\text{A5})$$

with $a_0 \geq a_3 \geq 0$ and $a_0^2 = a_3^2 = 1$. When this is rewritten as in (17), this implies that $\cos \frac{\theta}{2} \geq \sin \frac{\theta}{2} \geq 0$ which implies $\frac{\theta}{2} \in [0, \frac{\pi}{4}]$ and hence $\theta \in [0, \frac{\pi}{2}]$. We emphasize that (A5) is *not* the most general pure state of this “diagonal” form; instead $|\widehat{\psi}\rangle$ should be viewed as a canonical state from which all others with the same entanglement can be written as $(U^\dagger \otimes V^\dagger)|\widehat{\psi}\rangle$. We use the same notation as in (13) because the equivalence class of states defined by (12) corresponds exactly to the equivalence class of matrices with the same singular values.

In the form (A5) it is easy to find the entanglement of $|\psi\rangle$ because

$$\text{Tr}_1|\beta_0\rangle\langle\beta_3| = \text{Tr}_1|\beta_0\rangle\langle\beta_0|(I \otimes \sigma_3) = (\frac{1}{2}I_2)\sigma_3 = \frac{1}{2}\sigma_3 \quad (\text{A6})$$

Therefore, the reduced density matrix of (A5) is

$$\gamma = \frac{1}{2}(I + 2a_0 a_3 \sigma_3), \quad (\text{A7})$$

and its entanglement is $S(\gamma) = h(2a_0 a_3)$ where $h(x)$ is the binary entropy

$$h(x) \equiv -\frac{1+x}{2} \ln \frac{1+x}{2} - \frac{1-x}{2} \ln \frac{1-x}{2}. \quad (\text{A8})$$

In this paper we consider subfamilies of states of the form (A5) with UV^T fixed. When $UV^T = I$, $U = \overline{V}$ and the SVD becomes $V A V^\dagger$, which is the standard form for diagonalizing a self-adjoint matrix. Note that A is self-adjoint if and only if all a_k in (A2) are real and this property is preserved by the transformation $V A V^\dagger$. Thus, if we begin with a state $|\widehat{\psi}\rangle$ of the diagonal form (A5) with matrix $D = a_0 I + a_3 \sigma_3$, then the family of states

$$|\psi\rangle = (V^T \otimes V^\dagger)|\widehat{\psi}\rangle = (I \otimes V^\dagger D V)|\beta_0\rangle = (I \otimes A)|\beta_0\rangle \quad (\text{A9})$$

with V unitary all have real coefficients a_k when written in the form (A2).

Since any maximally entangled state can be written as $|\beta\rangle = (U_1 \otimes U_2)|\beta_0\rangle = (I \otimes U_2 U_1^T)|\beta_0\rangle$, the vector $|\beta_0\rangle$ can be regarded as the canonical representative of the equivalence class of maximally entangled states. This also gives a one-to-one correspondence between maximally entangled states and unitary matrices in M_2 via the relation

$$|\beta\rangle = (I \otimes U)|\beta_0\rangle = (U^T \otimes I)|\beta_0\rangle. \quad (\text{A10})$$

A matrix is unitary if and only if it can be written (up to an overall phase factor) as $U = u_0 I + i \sum_k u_k \sigma_k$ with u_k real. Thus, a state written in the form (A2) with a_0 real is maximally entangled if and only if $\text{Re } a_k = 0$ for $k = 1, 2, 3$.

APPENDIX B: COMPARISON LEMMAS

For $r_1 > r_2 > r_3$ it is elementary to verify that

$$\frac{1}{(r_1 - r_2)(r_1 - r_3)} + \frac{1}{(r_2 - r_1)(r_2 - r_3)} + \frac{1}{(r_3 - r_1)(r_3 - r_2)} = 0 \quad (\text{B1})$$

and

$$\frac{r_1}{(r_1 - r_2)(r_1 - r_3)} + \frac{r_2}{(r_2 - r_1)(r_2 - r_3)} + \frac{r_3}{(r_3 - r_1)(r_3 - r_2)} = 0 \quad (B2)$$

Lemma 6 Let $P(x) = -(x - r_1)(x - r_2)(x - r_3)$ be the cubic polynomial with real roots $r_1 > r_2 > r_3$ and let $Q(x) = P(x) + \delta_1 x + \delta_2$ with $\delta_1, \delta_2 > 0$. Then the roots of $Q(x)$ are approximately $s_k \approx r_k + \frac{1}{(r_m - r_k)(r_n - r_k)}(r_k \delta_1 + \delta_2)$ with k, m, n distinct.

Proof: Near each of the roots, the tangent to $P(x)$ is

$$y = (x - r_k)P'(r_k) = -(x - r_k) \frac{1}{(r_m - r_k)(r_n - r_k)} \quad (B3)$$

from which it follows that near $x = r_k$

$$Q(x) \approx -(x - r_k)(r_m - r_k)(r_n - r_k) + \delta_1 x + \delta_2. \quad (B4)$$

It then follows that $Q(s_k) \approx 0$ if

$$\begin{aligned} s_k &= r_k \frac{1}{1 - \frac{\delta_1}{(r_m - r_k)(r_n - r_k) - \delta_1}} + \frac{\delta_2}{(r_m - r_k)(r_n - r_k) - \delta_1} \\ &\approx r_k + r_k \frac{\delta_1}{(r_m - r_k)(r_n - r_k)} \\ &+ \frac{\delta_2}{(r_m - r_k)(r_n - r_k) - \delta_1}. \quad \text{QED} \end{aligned} \quad (B5)$$

Lemma 7 Let \mathbf{v} be a vector in \mathbf{R}_3 with all $v_1 > v_2 > v_3 > 0$ and let $v_k \mapsto w_k \equiv v_k + \frac{1}{(v_m - v_k)(v_n - v_k)}\epsilon v_k$. Then $\|\mathbf{w}\|_1 = \|\mathbf{v}\|_1$ and $\|\mathbf{w}\|_p > \|\mathbf{v}\|_p$ when $\epsilon > 0$ and $p > 1$.

Proof: The fact that $\|\mathbf{w}\|_1 = \|\mathbf{v}\|_1$ follows from (B2). For $p > 1$, observe that

$$\sum_k w_k^p = \sum_k v_k^p + p\epsilon v_k^{p-1} \frac{1}{(v_m - v_k)(v_n - v_k)}\epsilon v_k + O(\epsilon^2) \quad (B6)$$

Thus, up to $O(\epsilon^2)$,

$$\begin{aligned} \|\mathbf{w}\|_p^p - \|\mathbf{v}\|_p^p &= \epsilon p \left(\frac{v_1^p}{(v_1 - v_2)(v_1 - v_3)} - \frac{v_2^p}{(v_1 - v_2)(v_2 - v_3)} \right. \\ &\quad \left. + \frac{v_3^p}{(v_1 - v_3)(v_2 - v_3)} \right) \\ &= \epsilon p \frac{1}{v_1 - v_3} \left(\frac{v_1^p - v_2^p}{v_1 - v_2} - \frac{v_2^p - v_3^p}{v_2 - v_3} \right) \geq 0 \quad (B7) \\ &= \epsilon p^2 \frac{1}{v_1 - v_3} (v_1^{p-1} - v_3^{p-1}) \geq 0 \quad (B8) \end{aligned}$$

where we used (B1), and then the mean value theorem to obtain (B8) with $v_1 \geq \dot{v}_1 \geq v_2$ and $v_2 \geq \dot{v}_3 \geq v_3$. The inequality on the right in (B7) follows from the fact that

$f(x) = x^p$ is convex for $p > 1$. Although this suffices to prove the Lemma, the expression (B8), will be useful when we need to compare competing terms. **QED**

Lemma 8 Let \mathbf{v} be a vector in \mathbf{R}_3 with all $v_1 > v_2 > v_3 > 0$ and let $v_k \mapsto w_k \equiv v_k + \frac{1}{(v_m - v_k)(v_n - v_k)}\epsilon$. Then $\|\mathbf{w}\|_1 = \|\mathbf{v}\|_1$ and for $\epsilon > 0$

$$\|\mathbf{w}\|_p > \|\mathbf{v}\|_p \quad \text{for } p > 2 \quad (B9a)$$

$$\|\mathbf{w}\|_p < \|\mathbf{v}\|_p \quad \text{for } 1 < p < 2 \quad (B9b)$$

Proof: The proof is identical to that of Lemma 7 above except that (B7) becomes

$$\begin{aligned} \|\mathbf{w}\|_p^p - \|\mathbf{v}\|_p^p &= \epsilon p \frac{1}{v_1 - v_3} \left(\frac{v_1^{p-1} - v_2^{p-1}}{v_1 - v_2} - \frac{v_2^{p-1} - v_3^{p-1}}{v_2 - v_3} \right) \\ &= \epsilon p(p-1) \frac{1}{v_1 - v_3} (\dot{v}_1^{p-2} - \dot{v}_3^{p-2}) \end{aligned} \quad (B10)$$

where, as before $v_1 \geq \dot{v}_1 \geq v_2$ and $v_2 \geq \dot{v}_3 \geq v_3$. When $p > 2$, the function x^{p-1} is convex; however, when $1 < p < 2$, it is concave. Moreover, when $p-2 < 0$, the expression on the right in (B10) is negative because $\dot{v}_3 \leq v_2 \leq \dot{v}_1$. **QED**

$\mu < \mu_c$	$\mu \geq \mu_c$
$\frac{1}{4}(1-\mu)(1+\lambda^2) + \frac{\mu}{2} + \frac{1}{2}\sqrt{\frac{\mu^2}{1-\lambda^2} + (1-\mu)^2\lambda^2}$	$\frac{1}{4}(1-\mu)(1+3\lambda^2) + \mu$
$\frac{1}{4}(1-\mu)(1-\lambda^2)$	$\frac{1}{4}(1-\mu)(1-\lambda^2)$
$\frac{1}{4}(1-\mu)(1-\lambda^2)$	$\frac{1}{4}(1-\mu)(1-\lambda^2)$
$\frac{1}{4}(1-\mu)(1+\lambda^2) + \frac{\mu}{2} - \frac{1}{2}\sqrt{\frac{\mu^2}{1-\lambda^2} + (1-\mu)^2\lambda^2}$	$\frac{1}{4}(1-\mu)(1-\lambda^2)$

TABLE I: Optimal output eigenvalues for $p = 2$

APPENDIX C: EIGENVALUE COMPARISON

The eigenvalues of Δ are easy to find for the two boundary cases of $a = 0$ and $a = 1$. The lists in Table II are intended to be in decreasing order, but the two smallest eigenvalues may switch for very small M_μ . Although the largest eigenvalue is always greater for $a = 1$ than for $a = 0$, the same is also true for the smallest. This precludes using majorization to conclude that all p -norms for $a = 1$ exceeds that for $a = 0$. However, as discussed in Section V B, the eigenvalues for $a = 1$ could still trump those for any $a < 1$. If so, the optimal output eigenvalues for $p = 2$ given in Table I are conjectured to also be optimal for all $p > 1$.

$a = 0$	$a = 1$
$1 + \lambda^2 + \sqrt{4\lambda^2 - (1 - \lambda^2)S^2}$	$\nearrow 1 + \lambda^2 + \frac{1}{2}M_\mu + \sqrt{\frac{1}{4}M_\mu^2 + 4\lambda^2 - (1 - \lambda^2)S^2 + M_\mu \lambda S }$
$1 - \lambda^2 + M_\mu$	$\searrow 1 - \lambda^2$
$1 + \lambda^2 - \sqrt{4\lambda^2 - (1 - \lambda^2)S^2}$	$\nearrow 1 + \lambda^2 + \frac{1}{2}M_\mu - \sqrt{\frac{1}{4}M_\mu^2 + 4\lambda^2 - (1 - \lambda^2)S^2 + M_\mu \lambda S }$

TABLE II: Eigenvalues of Δ with arrows showing expected increase and decrease with a .

[1] C. H. Bennett and P. W. Shor, IEEE Trans. Inf. Th. **44**, 2724 (1998).

[2] C. Macchiavello and G. M. Palma, Phys. Rev. A **65**, 050301(R) (2002).

[3] C. Macchiavello, G. M. Palma and S. Virmani, Phys. Rev. A **69**, 010303(R) (2004).

[4] G. Bowen and S. Mancini, Phys. Rev. A **69**, 012306 (2004).

[5] N. J. Cerf, J. Clavareau, C. Macchiavello, and J. Roland, Phys. Rev. A **72**, 042330 (2005).

[6] V. Giovannetti, J. Phys. A **38**, 10989 (2005).

[7] V. Giovannetti and S. Mancini, Phys. Rev. A **71**, 062304 (2005).

[8] D. Kretschmann and R. F. Werner, Phys. Rev. A **72**, 062323 (2005).

[9] G. Ruggeri, G. Soliani, V. Giovannetti, and S. Mancini, Europhys. Lett. **70**, 719 (2005).

[10] D. Daems, Phys. Rev. A **76**, 012310 (2007).

[11] A. S. Holevo, paper presented at Quantum Informatics Symposium, Zvenigorod, 1-4.10.2002, eprint arXiv: quant-ph/0212025.

[12] A. S. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998)

[13] E. Karpov, D. Daems, N.J. Cerf, Open Sys. and Information Dyn. **13**, 363 (2006); E. Karpov, D. Daems, N.J. Cerf, Phys. Rev. A **74**, 032320 (2006).

[14] C. King and M.B. Ruskai, IEEE Trans. Inf. Theory **47**, 1-19 (2001).

[15] P. Shor, private communication. The additivity of minimal entropy was initially conjectured by P. Shor and circulated for some time. The first reference in print seems to have been in [14].

[16] G.G. Amosov, A.S. Holevo, and R.F. Werner, Probl. Inf. Transm. **36**, 305 (2001).

[17] P. W. Shor, Commun. Math. Phys. **246**, 453– 472 (2004).

[18] Hayden, eprint arXiv:0707.3291 (2007); Winter, eprint arXiv:0707.0402 (2007).

[19] R. Alicki and M. Fannes, Open Systems and Information Dynamics **11**, 339-342 (2004).

[20] M. Fukuda, J. Phys. A Math. Gen. **38**, L753-L758 (2005).

[21] C. King, J. Math. Phys. **43**, 4641 (2002).

[22] C. King, IEEE Trans. Inf. Th. **49**, 221 (2003).

[23] C. King and M.B. Ruskai, Quantum Information, Statistics and Probability, ed. by O. Hirota, 102–114 (World Scientific, 2004) eprint arXiv:quant-ph/0401026.

[24] S. Michalakis, J. Math. Phys. **48**, 122102 (2007).

[25] A. Rényi, “On measures of entropy and information” pp. 547–561 in *Proc. 4th Berkeley Sympos. Math. Statist. and Prob.*, Vol. I (Univ. California Press, Berkeley, 1961).

[26] S. Daftuar, “Eigenvalue Inequalities in Quantum Information Processing”, Caltech thesis (2004).

[27] S. Daftuar and M. Klimesh, Phys. Rev. A **64**, 042314 (2001).

[28] D. Jonathan, M.B. Plenio, Phys. Rev. Lett. **83**, 3566– 3569 (1999).

[29] G. Aubrun and I. Nechita, Commun. Math. Phys. **278**, 133-144 (2008).

[30] G. Aubrun and I. Nechita, eprint arXiv:0707.0211 (2007).

[31] R.A. Horn and C.R. Johnson, *Topics in Matrix Analysis* (Cambridge University press, 1991).

[32] Ky Fan, Proc. Nat. Acad. Sci. **37**, 760–766 (1951).

[33] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, Phys. Rev. A **54**, 3824-3851 (1996).